CYLERA™

SOLUTION BRIEF

Cylera for Higher Education

Advanced IoT Asset Intelligence and Security for Higher Education

The easiest, most accurate, and extensible platform for higher education IoT asset intelligence and security

The Challenge

Higher education institutions are increasingly targeted by sophisticated cyber threat actors focused on campus IoT devices. These adversaries seek to infiltrate campus networks, access sensitive institutional information like research data and student records, and disrupt academic operations.

Many vendors offer re-purposed, generalized IT technology solutions that fail to adequately safeguard uptime and manage critical IoT systems within specialized educational environments. These "wide but shallow" solutions lack the depth required to address complex IoT security challenges and operational requirements unique to higher education.

How Cylera Helps

The Cylera platform uses patented technology to monitor campus IoT devices with precision, offering real-time IoT device inventory, usage insights, risk prioritization, threat detection, remediation guidance, and support for network segmentation and zero trust tailored to educational settings. Institutions in higher education benefit from Cylera's customer-driven design, actionable insights, automated IoT device security monitoring and policy generation, and understanding of IT/SOC workflows. The platform also provides extensive integrations with leading SIEM, firewall, NAC, IT service management, and vulnerability management solutions to secure a diverse array of higher education IoT devices without disrupting campus activities.

Additionally, Cylera supports compliance with cybersecurity frameworks such as HIPAA in the US and GDPR in the UK, ensuring higher education organizations maintain secure, compliant campus operations.

Benefits

- **Enhanced Data Protection:** Safeguard sensitive research, student, and faculty data, reducing breach risk and ensuring compliance with higher education cybersecurity compliance standards and regulations.
- **Operational Resilience:** Minimize disruptions by proactively identifying and mitigating IoT risks, ensuring uninterrupted campus operations.
- **Cost Efficiency:** Optimize resource allocation and reduce financial losses related to cyber incidents or inefficient IoT asset management.
- **Improved Decision-Making:** Utilize advanced IoT device analytics to obtain actionable insights that enable institutions to make informed, strategic decisions.
- **Strengthened Reputation:** Demonstrate a commitment to cybersecurity to foster trust among students, faculty, and stakeholders.

Key Cylera Use Cases

- **IoT Discovery & Inventory:** Know and share what, where, and the operating state of your higher education IT and IoT devices. Discover previously unknown devices on your network. Avoid time consuming, inaccurate, out-of-date, and incomplete IoT asset records.
- **Vulnerability & Risk Management:** Gain operational awareness into higher education IoT devices across your network to improve your institution's security posture. Reduce data breach, reputation, disruption, privacy, compliance, and expenditure risks.
- **Threat Detection & Response:** Reduce alert noise, pinpoint actual security issues, and streamline remediation to speed higher education IoT threat response. Response prioritization, triage context, and prescriptive remediation guidance enable teams to resolve issues faster and more easily.
- **Network Segmentation & Protection:** Prevent unauthorized access and contain malware and other threats with automated network segmentation policy generation and integrations with firewall and NAC solutions. Detect and isolate risky IT and IoT devices that put research, student, and staff data at risk.
- **Analytics & Reporting:** Capture comprehensive higher education IT and IoT device inventory, security, and usage data to improve security, optimize device procurement and management, and enhance overall campus operations.
- **Compliance:** Obtain the higher education IoT visibility, inventory, risk, and threat management data required to support higher education audit and compliance requirements, including ISO/IEC 27001, HIPAA and FERPA in the US, and GDRP, NIS, and Cyber Essentials in the UK.

What Makes Cylera Unique

Rapid Time-to-Value: Easy to deploy, use, and expand usage backed by outcome-driven implementation and on-going engagement

Smart Monitoring: Real-time identification and classification of new and unknown higher education IoT assets without requiring other sources or retooling

High Fidelity Intelligence: Continuous, deep higher education IoT visibility, inventory, vulnerability, and telemetry details

True Risk Profiling: Scoring model using broad context for highly accurate vulnerability and threat detection, risk assessment, and prioritization to reduce alert noise and remediation lists

Efficient Threat Mitigation: Response prioritization, triage context, prescriptive remediation guidance, and segmentation policy generation help teams resolve issues faster and more easily

Comprehensive Analytics: Extensive higher education IoT asset operational data facilitates compliance and audit-readiness, and also enables allocation, procurement, hygiene, and governance

Cylera provides the easiest, most accurate and extensible platform for healthcare IoT intelligence and security to optimize patient care, service availability, and cyber defenses across diverse connected medical device and healthcare environments. The Cylera platform accurately discovers, categorizes, assesses, and monitors known and unknown assets with high fidelity to deliver unparalleled asset inventory, usage telemetry, risk prioritization, analytics, and guided threat remediation. Cylera integrates with popular IT and healthcare systems to allow organizations to advance cyber program maturity, increase operational efficiency,mitigate cyber threats, and enable compliance readiness.

CYLERA™

www.cylera.com